UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

CRIMINAL PRODUCTIONS, INC., Plaintiff, v. DOES 1-16, Defendants.	Civil Action No. 16-cv-1351 DECLARATION OF DANIEL ARHEIDT IN SUPPORT OF *EX PARTE* MOTION FOR EXPEDITED DISCOVERY

I, Daniel Arheidt, declare as follows:

1. My name is Daniel Arheidt. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I have been retained as a consultant by Maverickeye UG ("MEU"), a company incorporated in Stuttgart and organized and existing under the laws of Germany, in its technical department. MEU is in the business of providing forensic investigation services to copyright owners.

A. Peer-to-Peer Networks and the BitTorrent Protocol

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows users to freely and easily exchange ideas

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data. The Internet also affords opportunities for the wide-scale infringement of copyrighted motion pictures and other digital content. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet without significant degradation in picture or sound quality.

4. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called peer-to-peer ("P2P") or BitTorrent networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

5. To use a P2P or BitTorrent distribution system requires more than a click of a button. A substantial software installation and computer configuration process needs to take place. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material. The P2P systems represent a "viral" distribution or, in other words, systems that enable widespread distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that complete digital copies can be easily and quickly distributed thereby eliminating long download times.

6. Further, a person who uses a P2P network is free to use any alias (or "network name") whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

7. Additionally, the P2P methodologies for which MEU monitored for Plaintiff's motion picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file provider intentionally elects to share a file using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

8. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network can also be a source of download for that infringing file, potentially both copying and distributing the infringing work simultaneously. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent infringement.

B. Computer Forensic Identification of BitTorrent Infringement

9. All infringers connected to those files are investigated through downloading a part of the file placed on their computer. This evidence is then saved on a secure server. Once the forensic technology identifies an infringer in the way described herein for the motion picture for which Plaintiff owns the exclusive licensing and distribution rights, it automatically obtains the Internet Protocol ("IP") of a user offering the file for download and saves it in a secure database.

10. The forensic technology used by MEU is propriety software that collects, identifies and records the IP addresses in use by those people that employ the BitTorrent protocol to share,

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

copy, reproduce and distribute copyrighted works. In this way the software is connected to files of illegal versions of the motion picture.

11. An IP address is a unique numerical identifier that is automatically assigned to an Internet user by the user's Internet Service Provider ("ISP"). It only enables Plaintiff to trace the infringer's access to the Internet to a particular ISP. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet. Each time a subscriber logs on, he or she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet Assigned Numbers Authority ("IANA") or a regional internet registry such as the American Registry for Internet Numbers ("ARIN"). However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. These intermediaries can be identified by the ISP and the intermediaries own logs will contain the subscriber information.

12. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and other related information of the user/subscriber.

13. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of Internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

14. MEU determined that the Doe Defendants identified in Exhibit B to the complaint were using the ISPs to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

15. It is possible for digital files to be mislabeled or corrupted; therefore, MEU (and accordingly Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is being unlawfully distributed. This is done through a visual comparison between the version of the movie made available on file sharing networks by infringers and a control copy of Plaintiff's movie. Only when it is visually confirmed that the two movies are the same does monitoring for that version of the movie commence. To identify the IP Addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted motion picture, MEU's forensic software scans peer-to-peer networks for the presence of infringing transactions.

16. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the motion picture.

17. Through each of the transactions, the computers using the IP addresses identified in Exhibit B to the complaint transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit B. The IP addresses, hash values, dates and times and geolocation contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted motion picture.

18. Moreover, the users were sharing the exact same copy of the motion picture. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1." Using

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

hash tag to identify different copies of the motion picture, MEU is able to confirm that these users reproduced the very same copy of the motion picture.

19. The forensic software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit B using the SHA-1 algorithm. It verified that the piece(s) received by the monitoring system form part of Plaintiff's movie.

20. The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit B were located in the State of Washington. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial databases by ISPs. As set forth in Exhibit B to the complaint, I have confirmed not only that the users distributed the files in the State of Washington, but while not always precise with respect to physical location, I list further data indicating the estimated city in which the distribution took place.

21. Once provided with the IP address, plus the date and time of the infringing activity, the Doe Defendant's ISPs quickly and easily can use their respective subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time. However, ISPs typically retain user activity logs containing the information sought for only a limited period of time before erasing the data.

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct.

EXECUTED the 26 day of August, 2016.

Daniel Arheidt

LOWE GRAHAM JONES PLLC
701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301